Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6502
Transmittal Sheet
June 30, 2003

PRIVACY PROGRAM

1. REASON FOR ISSUE: To establish a Department-wide program for the protection of the privacy of veterans, their dependents and beneficiaries, as well as the privacy of all employees of the Department of Veterans Affairs (VA), and other individuals or entities for whom personal or entity specific records are created and maintained in accordance with Federal law.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive sets forth:

a. Policy for the Privacy Program. This policy requires VA-wide compliance with all applicable privacy law, regulations, Executive Orders and implementing policies, guidance, directives, and handbooks. This policy complies with Title 38 of the United States Code (U.S.C.) (U.S.C. 5701, 5705, 7332) and implementing VA regulations. Beyond Title 38, these policies are in accordance with the following Federal law, as embodied elsewhere in the U.S. Code, that bear directly on the privacy of personal data. The following list illustrates the various laws that contain privacy requirements and is not intended to be all-inclusive. This policy applies to all future amendments and all new privacy law: Fair Credit Reporting Act (1970) (Pub. L. 91-508); Privacy Act, as amended (1974) (Pub. L. 93-579); Right to Financial Privacy Act (1978) (Pub. L. 95-630); Electronic Communications Privacy Act (1986) (Pub. L. 99-508); Health Insurance Portability and Accountability Act (HIPAA) (1996) (Pub. L. 104-191); Gramm-Leach-Bliley Financial Modernization Act (1999) (Pub. L. 106-398); USA Patriot Act (2001) (Pub. L. 107-56); and E-Government Act of 2002 (Pub. L.107-347).

b. Policies for the Privacy Program are also in compliance with related Federal regulations such as the Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule), 45 CFR Parts 160 and 164, and the HIPAA Security Rule, 45 CFR Parts 160 and 164, both published by the Department of Health and Human Services (HHS). These policies also comply with Federal law related to the dissemination of Federal information, such as the Freedom of Information Act (FOIA).

c. Responsibilities for implementing and managing the Department-wide Privacy Program; and

d. References related to the Privacy Program.

3. RESPONSIBLE OFFICE: Office of Cyber and Information Security (005S), Office of the Assistant Secretary for Information and Technology (005).

4 RELATED HANDBOOK: None.

5. RESCISSIONS: None.

CERTIFIED BY:

/s/

John A. Gauss
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

John A. Gauss
Assistant Secretary for
Information and Technology

Distribution: RPC: 6002
FD

PRIVACY PROGRAM

1. PURPOSE and SCOPE

a. This directive establishes policies and responsibilities for the Department of Veterans Affairs (VA) Privacy Service and establishes the VA Privacy Program.

b. The VA Privacy Program shall apply to all personal data (herein referred to as "privacy-protected data") that is collected, created, transmitted, used, processed, stored, or disposed of (herein referred to as “maintained”) by, or for, VA regardless of the medium in which it resides or is transmitted.

c. The mission of VA is to serve America's veterans and their families. In order to fulfill this mission, it is necessary for VA to collect and maintain personal data about veterans, their dependents, and their beneficiaries, as well as collect and maintain such data for VA employees. The mission of the VA Privacy Service, through the implementation of the Privacy Program, is to preserve and protect the privacy of personal data gathered or created by VA in the course of performing official duties. The manner of this protection shall comply with requirements of all Federal statutes and regulations, Executive Orders, and Government and VA-wide policies, procedures, and guidance.

d. The provisions of this directive apply to all VA components and pertain to all privacy-protected data, which is maintained in any medium, including hard copy, microform, and electronic format, and by information systems administered by, or otherwise under the authority or control of, VA.

e. Terms used in this directive have their common meanings unless otherwise defined in the directive.

2. POLICY

a. VA shall implement a Department-wide Privacy Program through the establishment of a Privacy Service in the Office of Cyber and Information Security (OCIS).

b. VA shall ensure that all privacy-protected data that is maintained by, or for, VA in any medium, is kept confidential, except when disclosure is permitted or compelled under law.

c. The policy of VA is that privacy-protected data in the custody and control of VA shall be used and disclosed only as permitted or required by law.

d. VA shall perform Privacy Impact Assessments in compliance with the E-Government Act of 2002 (Pub. L. 107-347), and applicable Office of Management and Budget (OMB) guidance.

e. VA shall periodically assess compliance with all applicable privacy law. All VA entities that maintain privacy-protected data shall:

(1) Identify the privacy-protected data for which they are responsible;

(2) Comply with applicable Federal privacy law, regulations, and guidance pertaining to that privacy-protected data; and

(3) Submit a Privacy Review to the Privacy Service documenting the procedures used to comply with Federal privacy law and regulations.

f. VA personnel, contractors, and authorized users shall report all actual or suspected breaches of privacy in a timely and complete manner to agents designated by the Privacy Service. VA shall resolve all such issues of breach of privacy according to applicable law and in a timely fashion.

g. The physical input and output products of VA information systems that contain privacy-protected data, such as disks, paper, and compact disks (CD), shall be protected against misuse and unauthorized access, disclosure, modification, or destruction.

h. Security plans shall be developed and security controls implemented on the networks that transmit and store privacy-protected data. These controls shall be implemented, as required by law, to protect the security and privacy of the operating system, applications software, and data in VA information systems from accidental or malicious alteration or destruction, and to provide assurances to the user of the quality and integrity of VA maintained privacy-protected data.

i. VA shall provide periodic role-based privacy awareness training to all levels of VA staff.

j. VA shall assess and comply with new Federal privacy law, regulations, and guidance.

3. RESPONSIBILITIES

a. **The Secretary of Veterans Affairs.** The Secretary has designated the Assistant Secretary for Information and Technology as the Department's Chief Information Officer (CIO) who is the senior agency official responsible for the VA Cyber and Information Security and Privacy Programs.

b. **The Assistant Secretary for Information and Technology.** The Assistant Secretary for Information and Technology, as the VA CIO, shall:

(1) Establish Department-wide requirements, and provide oversight and guidance for all VA privacy protection issues;

(2) Designate the Associate Deputy Assistant Secretary (ADAS) for Cyber and Information Security as the principal Department official responsible for the VA Cyber and Information Security, and Privacy Programs, and assign the Director of the Privacy Service;

(3) Provide all VA privacy-protected reviews as required by applicable law;

(4) Develop and issue VA privacy directives, handbooks, and other Department-wide privacy publications, as appropriate;

(5) Establish a privacy training, education, and awareness program for all VA personnel and other authorized individuals involved in either the use and management of privacy-protected data, or the management, use, or operation of VA information systems containing these data; and

(6) Ensure that there are adequate staff and funding resources to properly fulfill all privacy-protection functions.

c. **The Associate Deputy Assistant Secretary (ADAS) for Cyber and Information Security.** The ADAS for Cyber and Information Security shall:

(1) Perform all privacy duties and responsibilities as designated by the CIO;

(2) Have overall responsibility for developing and implementing a Department-wide Privacy Program;

(3) Develop, issue, monitor, and implement VA privacy policies and procedures in accordance with Federal law and regulations;

(4) Issue technical guidance and direction to the Deputy CIOs and Privacy Officers regarding all aspects of implementing the Privacy Program at VA;

(5) Manage cyber security infrastructure activities to protect all privacy-protected data at VA;

(6) Provide for a system of privacy notifications, in accordance with applicable law, that pertain to all privacy-protected data;

(7) Issue guidance concerning the conduct and utilization of Privacy Reviews, and the contents of reports generated as a result of the Privacy Reviews;

(8) Facilitate cooperation in the VA Privacy Program among all VA Administrations, staff offices, and other key officials;

(9) Advise the VA CIO, Under Secretaries, Assistant Secretaries, and other key officials on privacy policy compliance, effective security controls over VA information systems, and other matters relevant to protecting all privacy-protected data and information systems carrying that data;

(10) Develop program spending plans that consider the risk to the integrity and confidentiality of all privacy-protected data on VA networks; and

(11) Develop multi-year plans to improve privacy controls as part of VA cyber and information security.

d. **Director, Privacy Service**. The Director shall:

(1) Develop, review, and coordinate privacy policy for VA in conjunction with policy efforts by all VA Administrations and staff offices;

(2) Coordinate Department-wide requirements, and monitor compliance with all Federal privacy law, regulations, and guidance;

(3) Establish Department-wide requirements for the responsibilities of Privacy Officers and provide implementation guidance, as needed;

(4) Establish Department-wide requirements and guidance on Privacy Rules of Behavior and monitor compliance with these requirements;

(5) Provide periodic Department-wide privacy awareness training and monitor compliance with this requirement;

(6) Provide Department-wide requirements on the development and implementation of periodic role-based privacy training;

(7) Require a Privacy Review, which is a review by Under Secretaries, Assistant Secretaries, other key officials, and data owners of all privacy-protected data for which they are responsible, and how such data is maintained;

(8) Review, monitor, and maintain the Privacy Reviews which shall be used to determine compliance with applicable law in conjunction with the Office of General Counsel;

(9) Analyze the existing safeguards to ensure the confidentiality of all privacy-protected data;

(10) Provide all required privacy-protected reporting, including recommendations to the ADAS for Cyber and Information Security, and the CIO, as required by applicable law;

(11) Examine new or pending legislation, in conjunction with the Office of General Counsel, to determine the actual or potential impact of such legislation on privacy policy and/or practice at VA; and

(12) Establish VA policy on the tracking and auditing of VA privacy violations and complaints by:

(a) Assigning, implementing, and managing a Department-wide system to track complaints and reports of alleged violations of applicable legal requirements providing for the privacy of individuals in VA;

(b) Maintaining audit records and documentation provided by the tracking system;

(c) Reporting to oversight agencies and VA management on privacy violation complaint resolution within VA, as required; and

(d) Providing oversight and guidance for VA compliance with applicable law relating to complaint and privacy-protected violations.

(13) Establish Department-wide requirements and guidance on the development and completion of Privacy Impact Assessments (PIA) by:

(a) Developing a PIA template for use on VA information systems;

(b) Providing oversight and monitoring compliance with the requirements of each PIA for each system; and

(c) Reporting results, as required by applicable law, to the CIO and oversight entities.

e. **The Inspector General**. This Office is responsible for:

(1) Conducting and supervising Privacy Program audits and providing follow-up regarding Privacy Program audit findings;

(2) Conducting or providing oversight for investigations concerning privacy-protected data; and

(3) Developing composite analyses of the assessments of risk to all privacy-protected data conducted as part of VA's Cyber and Information Security Program, identifying weaknesses, and recommending preventive measures and improvements.

(4) Nothing in this directive/Privacy Program shall prevent or impede the Inspector General from performing duties pursuant to the Inspector General Act or other statutory authority.

f. **The General Counsel**. This Office is responsible for:

(1) Interpreting laws, regulations, and directives applicable to VA privacy issues; and

(2) Rendering legal opinions on the compliance of each Administration with the privacy law applicable to that Administration by:

(a) Providing reviews of each Privacy Review for compliance with applicable law; and

(b) Rendering legal advice and services regarding privacy issues to Under Secretaries, Assistant Secretaries, and other key officials.

g. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials shall:

(1) Ensure that Department-wide privacy policies and procedures are implemented;

(2) Safeguard and secure all privacy-protected data stored or transmitted in VA information systems for which they are responsible, as well as those systems shared with, or operated by, other Federal agencies, contractors, or other outside organizations in coordination with the Office of Cyber and Information Security Privacy Program, and in accordance with Federal data security guidance;

(3) Work in close association with the Privacy Service to:

(a) Develop, implement, maintain, and enforce a structured program to adequately secure all privacy-protected data, and the systems and resources for which they are responsible; and

(b) Propose such regulations, issue such policy or guidance, and enter into such agreements as necessary to implement this directive.

(4) Assign to program offices the requirement to develop and submit to the Privacy Service a Privacy Review of all privacy-protected data for which they are responsible under applicable law, and describe how program offices maintain such privacy-protected data;

(5) Ensure that all employees and other authorized individuals under their respective jurisdictions act in compliance with the Department's privacy policies;

(6) Seek technical guidance and requirements for the protection of all privacy-protected data from the Director, Privacy Service, for the development and approval of cyber security acquisitions, budgeting, and funding;

(7) Appoint organizational Privacy Officers;

(8) Ensure that Privacy Officers report, in a timely manner, all actual or suspected breaches of privacy of all privacy-protected data to a tracking service designated by the Privacy Service for audit purposes;

(9) Allocate sufficient funds, personnel, and management support to implement the provisions of this directive, and ensure compliance with Federal and VA privacy program requirements;

(10) Ensure that personnel within their respective organizations attend privacy orientation and training in accordance with applicable legal requirements and guidance, Office of Personnel Management regulations, and VA privacy policy;

(11) Ensure that all personnel within their respective organizations attend initial privacy awareness and security training before they are granted access to any privacy-protected data, and that personnel receive follow-up privacy training periodically thereafter;

(12) Ensure that any reporting or notice requirements are met;

(13) Ensure that all alleged breaches of applicable Federal privacy law that, on their face, appear to constitute a criminal violation of law, are referred for investigation to the Office of the Inspector General;

(14) Ensure that noncompliance with these policies by VA personnel and other authorized individuals are addressed and remedied promptly including, if necessary, the initiation of penalties for non-compliance in accordance with applicable Federal law and VA personnel rules and regulations;

(15) Perform program reviews to assess the adequacy of privacy safeguards and identify weaknesses that would jeopardize the privacy and confidentiality of all privacy-protected data of VA personnel, veterans, and their dependents and beneficiaries; and

(16) Comply with all Departmental policy, procedures, and guidance concerning privacy.

4. REFERENCES

a. Computer Security Act of 1987, Pub. L. 100-235, 101 Stat. 1724, as amended.

b. Electronic Communications Privacy Act of 1986, as amended, Pub. L. 99-508, 100 Stat. 1848, 99th Cong. (October 21, 1986), codified at 18 U.S.C. 2510 et seq.

c. E-Government Act of 2002, Pub. L. 107-347.

d. Electronic Records Management, 60 Fed. Reg. 44634 (1995), 36 CFR Parts 12-20.

e. Fair Credit Reporting Act of 1970, Pub. L. 91-508.

f. Fraud and Related Activity in Connection with Access Devices and Computers, 18 U.S.C. 1029-1030.

g. Freedom of Information Act (FOIA), 38 CFR 1.550-557.

h. Gramm-Leach-Bliley Financial Modernization Act of 1999, Financial Services Modernization Act, Pub. L. 106-102, Title V, codified at 15 U.S.C. § 6801-6810.

i. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191.

j. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 CFR Parts 160 and 164.

k. National Institute for Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.

l. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.

m. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996.

n. Privacy Act of 1974, 38 CFR 1.575-582.

o. Right to Financial Privacy Act of 1978, Pub. L. 95-630.

p. Telephone Consumer Protection Act of 1991, Pub. L. 102-243.

q. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), Pub. L. 107-56, Title II.

r. VA Directive and Handbook 0710, Personnel and National Information Security.

s. VA Directive 6001, Limited Personal Use of Government Office Equipment Including Information Technology.

t. VA Handbook 6102, Internet/Intranet Services.

u. VA Directive 6103, VA Electronic Mail System.

v. VA Directive and Handbook 6210, Automated Information Systems Security.

w. VA Directive 6212, Security of External Electronic Connections.

x. VA Directive 6213, VA Public Key Infrastructure.

y. VA Directive 6214, VA Information Technology Security Certification and Accreditation Program.

z. VA Handbook 6300.2, Management of the Vital Records Program.

aa. VA Handbook 6300.3, Implementing the Freedom of Information Act (FOIA).

bb. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA).

cc. VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records.

dd. VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Addresses.

ee. VA Handbook 6300.8, Procedures for Shipment of Records to the VA Records Center and Vault in Neosho, Missouri.

ff. VA Handbook 6301, Procedures for Handling Electronic Mail Records.

gg. VA Handbook 6330, Directives Management Procedures.

hh. VA Handbook 6360.1, Procedures for Implementation of the Government Information Locator Service (GILS).

ii. 5 CFR Parts 731, 732, and 736.

jj. 38 U.S.C. 5701, Confidential Nature of Claims, 38 CFR 1.500-527.

kk. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records, 37 CFR 17.500-.511.

ll. 38 U.S.C. 7332, Confidentiality of Certain Medical Records, 38 CFR 1.460-.496.

5. DEFINITIONS

a. **Maintain.** Gather, create, use, store, disseminate, transmit, or dispose of privacy-protected data.

b. **Privacy-protected data.** All personal information that comes under the protection provisions of applicable Federal law and guidance.